Focus sur certaines applications du règlement eIDAS dans le domaine financier

Jacquemin, Hervé

Published in:
L'identification électronique et les services de confiance depuis le règlement eIDAS

Publication date:
2016

Document Version
le PDF de l'éditeur

Focus sur certaines applications du règlement eIDAS dans le domaine financier

Hervé Jacquemin* et Cathie-Rosalie Joly**

1.- Secteur financier et TIC. Les technologies de l'information et de la communication ne cessent de se développer et sont désormais omniprésentes dans la vie quotidienne des citoyens et des entreprises. Sans surprise, le domaine financier est également concerné et les professionnels du secteur (banques, compagnies d'assurance, entreprises de crédit, prestataires de services de paiements, etc.) y recourent de plus en plus pour promouvoir leurs services, conclure des contrats ou effectuer des opérations ponctuelles. Dans les relations avec leurs clients, la plupart des prestataires disposent ainsi d'un site internet et d'une application mobile, à des fins informatives ou transactionnelles. En interne, au niveau du back office, et dans les relations entre institutions financières, les technologies sont également utilisées.

La règlementation applicable au secteur financier est complexe et en constante évolution. On y trouve diverses exigences de forme, à respecter au moment de la formation des contrats ou en cours d'exécution (par exemple, pour y mettre fin) : écrit ou support durable, signature, mentions manuscrites, etc. Parallèlement, des modalités spécifiques de transmission de l'information peuvent être requises (lettre recommandée), tout comme des exigences de datation ou de conservation des documents. Enfin, des exigences fortes en termes d'authentification des utilisateurs peuvent être imposées aux prestataires (les banques, par exemple), notamment dans le cadre de paiements.

Aussi la question se pose-t-elle de savoir comment accomplir ces formalités, principales ou accessoires, dans l'environnement numérique.

Le règlement eIDAS apporte des réponses, qui modifient (sans le révolutionner) le cadre normatif actuellement applicable.

---

* Chargé d'enseignement à l'Université de Namur (CRIDS), chargé de cours invité à l'UCL et à l'ICHEC et avocat au barreau de Bruxelles.

** Chargée d'enseignement à l'Université Aix-Marseille III et Montpellier I et avocate aux barreaux de Paris et de Bruxelles.

2.- **Plan de la contribution**. Dans la présente contribution, on peut difficilement livrer une analyse exhaustive de toutes les applications possibles du règlement eIDAS dans le secteur financier.

Aussi nous limitons-nous à un examen ciblé des formes entourant la conclusion de deux contrats spécifiques, le contrat de crédit à la consommation et le contrat d'assurance (chapitre I), avant de nous pencher sur certaines questions ponctuelles spécifiques au secteur financier – paiements électroniques, dématérialisation du prélèvement SEPA et obligation d'identification des clients dans la lutte contre le blanchiment de capitaux (Chapitre II).

CHAPITRE I. Application du règlement eIDAS aux formalités entourant la conclusion des contrats

3.- **Conclusion des contrats par voie électronique et exigences de forme.** Eu égard à la faiblesse du consommateur de services financiers, le législateur mobilise en sa faveur divers mécanismes de protection, parmi lesquels figurent le renforcement des obligations d'information et la multiplication des exigences de forme (écrit, support durable, mentions manuscrites, exemplaires multiples, etc.)[1].

En général, ces exigences sont imposées dans la période contemporaine à la formation du contrat. L'objectif est en effet de garantir un consentement informé et réfléchi, tout en permettant au consommateur de disposer d'un support durable contenant diverses informations utiles en cours d'exécution du contrat.

Pour illustrer l'apport du règlement eIDAS au moment d'accomplir valablement les exigences de forme dans l'environnement numérique, nous analysons deux contrats : le contrat de crédit à la consommation et le contrat d'assurance.

L'accent est mis sur les seules formalités traitées par le règlement eIDAS. Pour les autres, nous renvoyons simplement au cadre normatif applicable par ailleurs, et aux commentaires généraux dont il a fait l'objet.

[1] Sur l'origine de la faiblesse et les moyens mobilisés pour y répondre, voy. H. JACQUEMIN, « Focus sur certains mécanismes de protection du consommateur de produits et services financiers en matière contractuelle », in *La protection du consommateur de produits et services financiers*, Limal, Anthemis, 2012, pp. 123 et s.

SECTION 1. – Conclusion d'un contrat de crédit à la consommation par voie électronique

4.- **Contrat de crédit et acte de cession de rémunération.** Les formalités entourant la conclusion proprement dite du contrat de crédit à la consommation figurent à l'article VII.78 du Code de droit économique (*infra*, § 1er). Des formalités sont également imposées avant la conclusion du contrat, en matière d'information précontractuelle (art. VII.70 et s. du CDE) mais elles consistent principalement en la fourniture d'information sur un support durable, ce qui n'est pas couvert par le règlement eIDAS. Aussi ne les examinons-nous pas dans la présente contribution. Nous ne verrons pas non plus les exigences de vérification de l'identité des consommateurs, imposées aux prêteurs. Pour celles-ci, il devrait être possible d'utiliser la carte d'identité électronique belge, en tant que moyen d'identification[2].

Le contrat de crédit à la consommation est en pratique accompagné d'un acte de cession de rémunération, soumis aux exigences formelles de l'article 27 de la loi du 12 avril 1965 concernant la protection de la rémunération des travailleurs. Partant du postulat que l'entreprise de crédit souhaite mettre en place un processus totalement dématérialisé, nous verrons s'il est possible de lever les obstacles formels prévus par cette disposition (§ 2).

§ 1. Le contrat de crédit à la consommation

A. Panorama des exigences de forme

5.- **Exigences formelles entourant la conclusion d'un contrat de crédit**. L'article VII.78 du Code de droit économique impose l'accomplissement de quatre formalités principales au moment de conclure le contrat de crédit.

Le contrat de crédit doit être établi sur un support durable. La notion est définie à l'article I.9, 22°, du Code de droit économique comme « tout instrument permettant à une personne de stocker des informations qui lui sont adressées personnellement d'une manière lui permettant de s'y reporter aisément à l'avenir pendant un laps de temps adapté aux fins auxquelles les informations sont destinées et qui permet la reproduction à l'identique des informations stockées ».

[2] Nous renvoyons aux contributions du présent ouvrage relatives à l'identification électronique, conformément au règlement eIDAS (en particulier celle de D. Gobert).

Le contrat doit contenir divers éléments. Il doit d'abord reprendre les conditions contractuelles et les mentions visées à l'article VII.78, §§ 2 à 4. Des mentions spécifiques doivent être écrites par le consommateur. Il doit en effet faire « précéder sa signature de la mention du montant total dû par le consommateur : « Lu et approuvé pour... euros à rembourser. ». [...] Le consommateur y apporte également la mention de la date et de l'adresse précise de la signature du contrat »[3] (art. VII.78, § 1er, al. 3, du CDE).

Toutes les parties contractantes doivent également apposer leur signature, l'article VII.78, § 1er, du Code de droit économique précisant que celle-ci peut être manuscrite ou électronique.

Enfin, un exemplaire du contrat de crédit doit être reçu par chaque partie contractante ayant un intérêt distinct et par l'intermédiaire de crédit[4].

6.- Formalités constituant des conditions de validité du contrat. Il est important de souligner que ces exigences formelles constituent des conditions de validité du contrat de crédit.

Plusieurs d'entre elles sont ainsi visées à l'article VII.195 du Code de droit économique, aux termes duquel « le juge annule le contrat ou réduit les obligations du consommateur au maximum jusqu'au prix au comptant ou au montant emprunté, lorsque le prêteur ne respecte pas les mentions visées à l'article VII.78, § 1er, alinéa 2, § 2, 5° à 9°, § 3, 1° à 7°, 11°, 13° et 14°.

Le juge peut prendre une mesure similaire lorsque le prêteur :

1° ne respecte pas les mentions visées à l'article VII.78, § 2, 1° à 4°, § 3, 8° à 10°, 12° et 15° [...] ».

S'agissant de la signature, il faut avoir égard à l'article VII.90, alinéa 1er, du Code de droit économique, qui interdit tout paiement par le prêteur au consommateur (ou pour le compte de celui-ci) ou par le consommateur au prêteur aussi longtemps que le contrat de crédit n'a pas été signé par toutes les parties. La sanction civile est particulièrement sévère pour le prêteur puisque, si une somme est versée en méconnaissance de cette interdiction (voire un bien ou un service fourni), « le consommateur n'est pas tenu de restituer la somme versée, de payer le service ou le bien ni de restituer ce dernier »[5].

[3] S'agissant d'une ouverture de crédit, la mention est un peu différente : « Lu et approuvé pour... euros à crédit ».

[4] Voy. aussi l'article VII.78, § 1er, alinéa 2, aux termes duquel, « sauf pour l'ouverture de crédit, aucun contrat de crédit à durée déterminée avec amortissement du capital n'est parfait tant qu'un tableau d'amortissement, visé au § 3, 4° du présent article, n'a pas été remis à chaque partie contractante ayant un intérêt distinct ».

[5] Art. VII.198 du CDE.

Pour les autres formalités (exemplaires multiples du contrat de crédit, mentions manuscrites, support durable), l'absence de sanction civile spécifique ne doit pas empêcher l'application des mesures tirées de la théorie générale des contrats et des obligations[6]. Dès lors que l'objectif des exigences de forme est clairement de protéger le consommateur, eu égard à sa faiblesse vis-à-vis du prêteur, il paraît cohérent d'admettre que la nullité prétorienne du contrat puisse être prononcée par le juge, s'il est démontré que le non-respect de l'exigence a porté atteinte aux intérêts du consommateur[7].

7.- Application du règlement eIDAS pour lever les obstacles formels ? Les mentions informatives peuvent être accomplies sans difficulté particulière dans l'environnement numérique (elles ne constituent pas un obstacle formel). De même, en utilisant la notion de « support durable » plutôt que le terme « écrit », le législateur opte pour une terminologie technologiquement neutre et susceptible de s'appliquer à des procédés traditionnels (le papier) ou numérique (un document au format pdf, par exemple)[8]. Dès lors que cet élément n'est pas visé par le règlement eIDAS, nous ne l'examinerons pas davantage.

S'agissant des exemplaires multiples de contrat ou de la remise d'un tableau d'amortissement, on peut se référer à la clause transversale générale de l'article XII.15, § 1er, du Code de droit économique, qui consacre la théorie des équivalents fonctionnels. Sur ce point également, le règlement eIDAS est normalement sans incidence.

[6] H. Jacquemin, « Focus sur certains mécanismes de protection du consommateur de produits et services financiers en matière contractuelle », *op. cit.*, pp. 123 et s., nos 18 et s.

[7] Pour une application dans le secteur financier, voy. Bruxelles, 16 mars 2009 (*D.B.F.*, 2009, p. 237, *J.T.*, 2009, p. 757, *R.G.D.C.*, 2010, p. 353, note H. Jacquemin, *R.D.C.*, 2011, p. 338, note A. André-Dumont), qui a décidé que « la sanction du défaut d'écrit conforme à la loi n'est pas prévue par le texte légal mais dans la mesure où cette formalité vise à protéger les clients, la partie faible au contrat, ce défaut de validité formelle doit être sanctionné par la nullité relative par application de la théorie générale des nullités ». Dans cette affaire, la cour d'appel de Bruxelles devait se prononcer sur la violation des exigences formelles prescrites par l'arrêté royal du 5 août 1991 relatif à la gestion de fortune et au conseil en placement. Cet arrêté royal a été abrogé et remplacé par l'arrêté royal du 3 juin 2007 ; cependant, les règles de forme à respecter se recouvrent, quel que soit le texte envisagé (l'A.R. du 5 août 1991 ou celui du 3 juin 2007) et, de manière identique, sont dépourvues de sanction civile expressément prévue par celui-ci. Voy. aussi, en matière de contrat de voyage, Cass., 26 mai 2006, *D.C.C.R.*, 2007, p. 196, note P. Wéry, *J.L.M.B.*, 2007, p. 339, *Pas.*, 2006, liv. 5-6, p. 1216, *R.G.D.C.*, 2007, p. 476, note P. Wéry ; Anvers, 21 février 2007, *D.C.C.R.*, 2008, p. 49, note H. De Coninck ; Anvers, 23 novembre 2004, *D.C.C.R.*, 2005, p. 41, note F. Van Bellinghen.

[8] À propos du support durable, voy. C.J.U.E., 5 juillet 2012, aff. C-49/11, *Content Services Ltd.* Pour un commentaire de cet arrêt, voy. H. Jacquemin, « Arrêt 'Content Services' : l'exigence du support durable dans les contrats à distance », *J.D.E.*, 2012, pp. 243-246 ; S. de Pourcq, « De informatieverplichting bij verkoop op afstand : een hyperlink die naar een gewone website leidt, volstaat niet », note sous C.J.U.E., 5 juillet 2012, *D.C.C.R.*, 2012/4, pp. 57 et s.

Il reste la signature et les mentions manuscrites, pour lesquelles le règlement eIDAS peut s'appliquer. Aussi les étudions-nous plus en détails.

B. Signature électronique

8.- Valse-hésitation du législateur belge. Par le passé, le recours à des procédés de signature électronique pour conclure des contrats de crédit à la consommation a fait l'objet de modifications normatives diverses, ce qui traduit les hésitations du législateur en la matière.

Avant d'être intégré – avec des amendements – dans le Code de droit économique[9], l'article 14, § 1er, de la loi du 12 juin 1991 sur le crédit à la consommation était rédigé comme suit : « le contrat de crédit est conclu par *la signature* de toutes les parties contractantes et est établi sur un support papier ou sur un autre support durable. Toutes les parties contractantes ayant un intérêt distinct ainsi que l'intermédiaire de crédit reçoivent un exemplaire du contrat de crédit » (nous soulignons). Aucun procédé de signature électronique n'était *a priori* exclu et, pour connaître les effets attachés au procédé utilisé (plus précisément pour savoir s'il pouvait être jugé équivalent à une signature manuscrite valable), il convenait de se référer à la clause transversale particulière de l'article XII.15, § 2, du Code de droit économique[10], qui renvoyait à la signature électronique qualifiée[11] ou à la signature électronique de l'article 1322, alinéa 2, du Code civil. S'agissant de formalités requises *ad validitatem*, le « détour » par la clause transversale particulière s'imposait.

Lors de l'introduction de l'article VII.78, § 1er, dans le Code de droit économique, en 2014, une modification a été apportée à la disposition, réduisant les procédés susceptibles d'être utilisés : dans l'environnement numérique, seule la signature électronique qualifiée était en effet visée[12].

[9] Loi du 19 avril 2014 portant insertion du livre VII « Services de paiement et de crédit » dans le Code de droit économique, portant insertion des définitions propres au livre VII et des peines relatives aux infractions au livre VII, dans les livres I et XV du Code de droit économique, et portant diverses autres dispositions, *M.B.*, 28 mai 2014.

[10] Auparavant, il s'agissait de l'article 16 de la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information (qui n'a pas été modifié lors de son intégration dans le livre XII du CDE).

[11] Plus précisément, il s'agissait de la signature électronique visée à l'article 4, § 4, de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification.

[12] En réalité, l'article VII.78, § 1er, du CDE renvoyait à l'article XII.25, § 4, du CDE. Cette référence était pour le moins maladroite dans la mesure où le projet d'article XII.25, § 4, n'a jamais été adopté. Il figurait dans une proposition de loi du 15 avril 2013 modifiant la législation en ce qui concerne l'instauration du droit de l'économie électronique (*Doc. Parl.*, Ch. repr., sess. ord. 2012-2013, n° 2745/001), qui est devenue caduque avec la dissolution

Les travaux préparatoires n'apportent malheureusement aucune explication à ce propos. Elle paraît difficilement compréhensible, lorsque l'on se souvient que l'article 14, § 1er, de la loi du 12 juin 1991 relative au crédit à la consommation avait déjà été modifié en 2010[13] en vue de permettre le recours à l'électronique. Les travaux préparatoires indiquaient à ce propos que « on a profité de l'occasion pour rendre également possible le crédit électronique en supprimant chaque référence aux mots "manuscrit" ou "mention manuscrite". La signature peut également se réaliser de manière électronique. L'actuel article 14, § 1er, alinéa 2, LCC a été abrogé car il prête à confusion et est imprécis »[14].

Par la suite, le législateur est cependant revenu sur sa position de 2014 et il a amendé l'article VII.78 par une loi du 26 octobre 2015 modifiant le Code de droit économique et portant diverses autres dispositions normatives[15]. Un quatrième alinéa a été ajouté à cette disposition. Il prévoit que « la signature électronique visée à l'alinéa 1er se fait :

- par une signature électronique avancée réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique, visée à l'article 4, § 4, de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification,
- ou par une autre signature électronique qui satisfait aux critères que le Roi peut fixer afin de garantir l'identité des parties, leur consentement sur le contenu du contrat de crédit et le maintien de l'intégrité de ce contrat. En cas de contestation, il incombe au prêteur de démontrer que cette signature électronique garantit effectivement ces fonctions ».

Dans les travaux préparatoires de la loi du 26 octobre 2015, on peut lire que « la loi du 19 avril 2014 qui insère le livre VII dans le Code de droit économique a apporté une modification importante par rapport aux dispositions de l'article 14 de la loi du 12 juin 1991 relative au crédit à la consommation. L'article 14, qui traite de la conclusion du contrat de crédit, imposait la signature des parties mais n'indiquait pas clairement si ce contrat pouvait être conclu par voie électronique. Désormais, l'article VII.78 ouvre cette possibilité »[16]. Cet argument est pour le moins étonnant lorsqu'on se souvient que la suppression du terme « manuscrite »

du Parlement en mai 2014). On comprend néanmoins que la disposition correspondante, actuellement en vigueur, est l'article 4, § 4, de la loi du 9 juillet 2001, qui désigne la signature électronique qualifiée.

[13] Loi du 13 juin 2010 modifiant la loi du 12 juin 1991 relative au crédit à la consommation.

[14] *Doc. Parl.*, Ch. repr., sess ord. 2009-2010, n° 2468/001, p. 35.

[15] *M.B.*, 30 octobre 2015, en vigueur le 9 novembre 2015.

[16] *Doc. parl.*, Ch. repr., sess. ord. 2014-2015, n° 1300/001, p. 12.

avait précisément pour but d'autoriser toute forme de signature, manuscrite ou électronique.

Dans sa version du 11 décembre 2015, l'avant-projet de loi mettant en œuvre et complétant le règlement eIDAS[17], actualise la référence à la signature électronique qualifiée, en renvoyant à l'article 3.12 du règlement eIDAS, et plus à l'article 4, § 4, de la loi du 9 juillet 2001, qui est abrogée[18]. Il permet également de signer le contrat de crédit au moyen d'un cachet électronique qualifié, tel que visé à l'article 3.27 du règlement.

9.- Que penser des formes de signature électronique visées par l'article VII.78, § 1er, du Code de droit économique ? Désormais, deux formes de signature électronique sont théoriquement admises par l'article VII.78, § 1er, du Code de droit économique pour la conclusion du contrat de crédit à la consommation : une signature électronique qualifiée (telle que visée par l'article 4, § 4, de la loi du 9 juillet 2001, puis par l'article 3.12 du règlement eIDAS) ou une autre signature électronique, qui doit remplir les fonctions d'identification des parties, de consentement au contenu du contrat de crédit et de maintien de l'intégrité de ce contrat, suivant des critères que le Roi peut fixer.

En ce qu'elle permet aux entreprises de crédit d'utiliser une autre forme de signature électronique que la signature électronique qualifiée (concrètement, dans la majorité des cas la signature électronique créée par la carte d'identité électronique), cette disposition doit assurément être approuvée. Les travaux préparatoires partent ainsi du constat que, dans le régime antérieur, les entreprises de crédit devaient soit renoncer à conclure des contrats de crédit à la consommation à distance, soit permettre l'utilisation de la carte d'identité électronique pour signer ceux-ci, avec les charges administratives et financières qui en résultent[19]. Or, le législateur note que « les établissements financiers ou de crédit ont développé, pour la signature d'opérations à distance, leurs propres systèmes relativement sécurisés et dont certains sont susceptibles d'assurer une protection suffisante de la transaction et du consommateur (tels que lecteurs de cartes ou digipass). En utilisant ces système, le client n'appose toutefois pas une

[17] Avant-projet de loi mettant en œuvre et complétant le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII « Droit de l'économie électronique » du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique.

[18] Art. 29 de l'avant-projet de loi.

[19] *Doc. parl.*, Ch. repr., sess. ord. 2014-2015, n° 1300/001, p. 13.

signature électronique qualifiée au sens légal du terme, ce qui serait donc contraire à la disposition de l'article VII.78 CDE »[20].

Sur le fond et la forme, les exigences imposées à cette autre forme de signature électronique nous paraissent néanmoins discutables à plusieurs égards.

Sur le fond, les fonctions attendues du second procédé de signature électronique nous paraissent très contestables, dans la mesure où elles ne correspondent pas aux fonctions généralement attribuées à la signature manuscrite. Pour celle-ci en effet, le maintien de l'intégrité du contenu de l'acte n'est pas requis. Aussi sommes-nous d'avis que le législateur crée une différence de traitement entre l'électronique et le papier, contraire au principe d'égalité et de non-discrimination. Une telle différence de traitement avait déjà été constatée pour l'article 1322, alinéa 2, du Code civil[21]. Cette différence de traitement est d'autant moins justifiée qu'elle est redondante par rapport aux fonctions du support durable, également requis pour la conclusion du contrat de crédit. Au nombre des fonctions attendues de celui-ci figure en effet le maintien de l'intégrité du contenu (l'instrument devant en effet, suivant la définition de l'article I.9, 22°, permettre « la reproduction à l'identique des informations stockées »)[22].

En pratique, cette fonction de maintien de l'intégrité du contenu pourrait poser de sérieuses difficultés. Dans un système de cryptographie asymétrique, elle exige en effet la création d'un condensé (hash) du message (le contrat en l'occurrence), qui est signé avec la clé privée du signataire, et dont on vérifie ensuite la conformité en le décryptant avec sa clé publique. Or, si les systèmes de lecteurs de cartes ou de digipass remplissent assurément une fonction d'identification et d'adhésion à l'opération signée au moyen de ceux-ci, il faudrait vérifier s'ils permettent également de préserver l'intégrité du contenu de l'acte. À défaut, la disposition légale dans sa mouture actuelle ne permettrait pas nécessairement d'atteindre les objectifs envisagés par le législateur.

On s'interroge également sur la délégation donnée au Roi en vue d'établir des critères garantissant les trois fonctions. À ce stade, aucun arrêté royal n'a été adopté. Si cette situation persiste, cela signifie-t-il que la disposition ne peut sortir aucun effet ? On peut le craindre même si l'intervention du Roi semble considérée comme une simple possibilité (et non une obligation – « le Roi peut »), et dès lors que les fonctions attendues sont déjà énumérées. Dès son adoption, il faudra en tout cas s'assurer que

[20] *Ibid.*

[21] Pour d'autres considérations en ce sens, voy. la contribution de B. Losdyck dans le présent ouvrage.

[22] En ce sens, voy. aussi C.J.U.E., 5 juillet 2012, aff. C-49/11, *Content Services Ltd.*

les critères ainsi établis n'ont pas pour effet d'alourdir les exigences attendues du procédé de signature, à l'aune des trois fonctions citées.

Enfin, on comprend mal la dernière phrase, suivant laquelle « en cas de contestation, il incombe au prêteur de démontrer que cette signature électronique garantit effectivement ces fonctions ». Le législateur semble envisager l'hypothèse d'un consommateur qui introduirait un recours en justice en vue de contester sa signature électronique, alors même qu'elle répondrait aux critères fixés par le Roi. Il opère un renversement de la charge de la preuve, jugeant démesuré de faire peser celle-ci sur le consommateur[23]. On peut toutefois s'interroger sur l'intérêt de fixer des conditions – probablement – lourdes dans un arrêté royal, qui n'offre finalement aucune sécurité juridique aux prêteurs (puisqu'ils devront quand même apporter la preuve que les trois fonctions ont été préservées.

Sur la forme, les fonctions attendues du procédé de signature électronique – identification des parties, consentement au contenu du contrat et maintien de l'intégrité – correspondent aux fonctions de la signature électronique énumérées à l'article 1322, alinéa 2, du Code civil. Pour rappel, cette disposition impose une double fonction d'imputabilité (dont on considère généralement qu'elle renvoie aux fonctions traditionnelles de la signature – soit l'identification ou, plus précisément l'authentification de l'identité et l'adhésion au contenu de l'acte) et de maintien de l'intégrité du contenu de l'acte[24]. Aussi eût-il été plus simple de renvoyer directement à l'article 1322, alinéa 2, du Code civil, tout en supprimant la référence à l'arrêté royal. On évitait ainsi de créer une nouvelle forme de signature électronique, au risque de compliquer inutilement le dispositif. Plus simplement encore, on pouvait faire l'économie de cette double référence à la signature électronique qualifiée ou à la signature électronique remplissant les trois fonctions précitées, en appliquant directement la clause transversale particulière de l'article XII.15, § 2, relative à la signature et qui renvoie à la signature électronique qualifiée ou à la signature électronique de l'article 1322, alinéa 2, du Code civil. Il est vrai que telle ne semble pas être la volonté du législateur, qui préfère imposer des conditions additionnelles, par arrêté royal, à cette autre forme de signature.

De lege ferenda, nous sommes d'avis que l'article VII.78, § 1er, devrait se limiter à exiger une signature manuscrite ou électronique (le dernier alinéa ajouté en octobre 2015 devrait par conséquent être supprimé). Par

[23] *Doc. parl.*, Ch. repr., sess. ord. 2014-2015, n° 1300/001, p. 13.

[24] Voy. en ce sens la contribution de H. Jacquemin ou de B. Losdyck, dans le présent ouvrage.

application de l'article XII.15, § 2, du Code de droit économique, on peut identifier les procédés de signature électronique équivalents à la signature manuscrite. Par ailleurs, l'article 1322, alinéa 2, du Code civil, devrait être amendé en vue de supprimer la fonction de maintien de l'intégrité du contenu de l'acte.

C. Mentions du consommateur

10.- Equivalents fonctionnels aux mentions du consommateur. Si le terme « manuscrit » ne figure pas à l'article VII.78, § 1er, alinéa 3, du Code de droit économique, pour qualifier les mentions qui doivent être apposées par le consommateur lors de la signature du contrat de crédit, il paraît évident que, dans l'environnement papier, la formalité se matérialisera par une mention écrite à la main par le débiteur.

Pour trouver l'équivalent fonctionnel à cette formalité dans l'environnement numérique, on peut se référer à la clause transversale particulière de l'article XII.15, § 2, du Code de droit économique, suivant laquelle « l'exigence d'une mention écrite de la main de celui qui s'oblige peut être satisfaite par tout procédé garantissant que la mention émane de ce dernier ».

Le verbe « émaner », utilisé par le législateur, semble exiger la réunion de deux conditions. Il faut *d'abord* que la mention soit rédigée par celui qui s'oblige. Une intervention active de sa part est requise. Concrètement, la partie faible peut être invitée à dactylographier le texte, au moyen du clavier de son ordinateur, dans une zone déterminée, sur une page du site web du prestataire. *Ensuite*, il faut nécessairement garantir que l'auteur de la mention est effectivement la partie faible, et pas son cocontractant (ou un tiers). C'est la fonction d'authentification de l'origine. Dans l'environnement traditionnel, la personnalisation du graphisme remplit cette fonction. En général, cette caractéristique n'existe pas dans l'environnement numérique : le recours au clavier de l'ordinateur conduit en effet à uniformiser le graphisme. Un procédé complémentaire doit être mis en œuvre et, à nos yeux, un mécanisme de signature électronique pourrait convenir.

11.- Recours à un procédé de signature électronique. Le système devrait donc être conçu de telle sorte que le procédé de signature électronique utilisé par ailleurs pour signer le contrat, soit également lié à la mention du consommateur.

Ce faisant, on exploite utilement les fonctions d'authentification de l'origine qu'offrent en pratique les procédés de signature électronique.

Elles résultent d'ailleurs très clairement des conditions à satisfaire, conformément au règlement eIDAS, pour qu'un procédé soit considéré comme une signature électronique avancée[25] ou une signature électronique qualifiée[26].

§ 2. L'acte de cession de rémunération

12.- Exigences formelles de l'acte de cession de rémunération. Lors de la conclusion d'un contrat de crédit, les prêteurs veillent à se ménager une sûreté en demandant au consommateur de compléter un acte de cession de rémunération. Celui-ci est visé à l'article 27 de la loi du 12 avril 1965 concernant la protection de la rémunération des travailleurs, aux termes duquel :

> *« La cession de la rémunération doit être faite par un acte distinct de celui qui contient l'obligation principale dont elle garantit l'exécution.*
> *Cet acte est établi en autant d'exemplaires qu'il y a de parties ayant un intérêt distinct.*
> *Dans les cas d'application de la loi du 12 juin 1991 relative au crédit à la consommation, l'acte doit reproduire les dispositions des articles 28 à 32.*
> *Les dispositions du présent article sont prescrites à peine de nullité ».*

Il est important de noter que ces exigences constituent des conditions de validité de l'acte de cession, au sens de *negotium* (accord de volontés). On rappelle en effet qu'il s'agit de dispositions impératives qui instaurent un formalisme de protection[27]. Ce ne sont donc pas des formalités probatoires, dont le non-respect affecterait uniquement l'*instrumentum* (sans incidence sur la convention en tant que telle)[28].

[25] *Cf.* art. 3.11 et art. 26 du règlement eIDAS.

[26] *Cf.* art. 3.12 et art. 28 et s. du règlement eIDAS.

[27] M. Forges, obs. sous Cass., 10 février 1997, *J.T.T.*, 1997, p. 280.

[28] Dans un arrêt du 10 février 1997 (*Pas.*, 1997, I, p. 195), la Cour de cassation a ainsi décidé que « la formalité prescrite à peine de nullité, suivant laquelle l'acte de cession de la rémunération doit être établi en autant d'exemplaires qu'il y a de parties ayant un intérêt distinct, ne concerne pas la réglementation de la preuve mais vise la protection du cédant, afin de lui permettre de vérifier la portée de son obligation, de sorte qu'une copie de l'acte de cession, sur laquelle figure une signature du cédant obtenue au moyen d'un papier carbone, constitue un exemplaire au sens de la formalité précitée ». De même, dans un arrêt du 17 novembre 2008 (*J.T.T.*, 2009, p. 83), elle a confirmé le caractère strict du formalisme, en cassant la décision qui avait refusé de sanctionner l'absence de mentions, sous prétexte que le consommateur était parfaitement informé de la portée de ses obligations. Elle décide en effet qu'« il résulte de cette disposition et de l'intention du législateur de protéger efficacement le cédant que l'acte de cession doit indiquer l'obligation principale dont l'exécution est garantie ainsi que le montant pour lequel la cession est consentie ». Même si l'objectif des mentions est visiblement atteint en l'espèce, la Cour de cassation refuse que leur méconnaissance ne soit pas sanctionnée

13.- Comment accomplir valablement ces formalités dans l'environnement numérique ? Pour les exigences consistant à reproduire des *mentions*, faire en sorte que l'acte soit *distinct* et établi en *plusieurs exemplaires*, on ne rencontre normalement pas de difficulté particulière dans l'environnement numérique. S'agissant en particulier de l'exigence d'exemplaires multiples, on se rappellera de l'interprétation donnée par la Cour de cassation, qui juge qu'il ne faut pas respecter les mêmes exigences que conformément à l'article 1325 du Code civil. Cette disposition impose en effet des originaux ; or, pour l'application de la loi du 12 avril 1965, la Cour de cassation se suffit de copies carbone, qui ne constituent pas des originaux, sur lesquels la signature a été directement apposée[29].

Par contre, l'exigence d'un « acte » constitue un obstacle formel qui doit être levé pour que la cession de rémunération puisse être dématérialisée. La doctrine considère généralement que le terme est synonyme d' « écrit »[30]. Dès lors que l'acte de cession de rémunération doit constater la manifestation de la volonté du consommateur de céder sa rémunération en cas de non-respect de ses engagements dans le cadre du contrat de crédit, l'acte doit également être revêtu de la signature du débiteur. C'est confirmé par le fait que le terme « acte » désigne aussi l'accord de volontés (le *negotium*)[31].

En l'occurrence, on ne peut toutefois pas se référer aux clauses transversales particulières relatives à l'écrit et la signature, telles que prévues à l'article XII.15, § 2, du Code de droit économique, pour déterminer les fonctions de la formalité et, ainsi, identifier un procédé fonctionnellement équivalent susceptible d'être mis en œuvre dans l'environnement numérique. Conformément à l'article XII.16, 3°, du Code de droit économique, il faut en effet exclure de l'application de l'article XII.15 « les contrats de sûretés et garanties fournis par des personnes agissant à des

[29] Cass., 10 février 1997, *Pas.*, 1997, I, p. 195.

[30] Assimilant l'acte à l'écrit, H. De Page, *Traité élémentaire de droit civil belge*, t. III, 3e éd., Bruxelles, Bruylant, 1967, p. 794, n° 777 ; N. Verheyden-Jeanmart, *La preuve*, Bruxelles, Larcier, 1991, p. 194, n° 396 ; D. Gobert et E. Montero, « L'ouverture de la preuve littérale aux écrits sous forme électronique », *J.T.*, 2001, p. 122 ; P. Lecocq et B. Vanbrabant, « La preuve du contrat conclu par voie électronique », *Le commerce électronique : un nouveau mode de contracter*, Liège, Éd. du Jeune Barreau, 2001, p. 69, n° 23 ; D. Mougenot, *La preuve*, 3e éd., tiré à part du *Rép. not.*, Bruxelles, Larcier, 2002, p. 138, n° 80. Voy. aussi le rapport fait au nom de la Commission de la Justice par B. Somers, relatif à la proposition de loi introduisant de nouveaux moyens de télécommunication dans la procédure judiciaire et extrajudiciaire, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000 (lég. 50), n° 38/008, p. 25.

[31] D. Mougenot, *La preuve*, *op. cit.*, pp. 138-139, n° 80.

fins qui n'entrent pas dans le cadre de leur activité professionnelle ou commerciale ».

14.- Application du règlement eIDAS, en espérant une modification législative. Cette exclusion des sûretés ne nous paraît pas justifiée[32] : comme pour le cautionnement à titre gratuit visé à l'article 2043*quinquies* du Code civil[33] (pour lequel on ne peut pas trouver d'équivalent fonctionnel à la mention manuscrite en se fondant sur l'article XII.15, § 2[34]), on ne voit pas pourquoi il n'est pas possible de se fonder sur les clauses d'assimilation de l'article XII.15 du Code de droit économique. *De lege ferenda*, nous sommes d'avis que cette exclusion devrait, purement et simplement, être supprimée.

[32] Seule l'hypothèse visée à l'article XII.16, 2° (« les contrats pour lesquels la loi requiert l'intervention des tribunaux, des autorités publiques ou de professions exerçant une autorité publique »), nous semble pertinente. Les exclusions définies à l'article XII.16, 1°, 3° et 4°, qui reprennent littéralement les hypothèses de l'article 9, § 2, de la directive sur le commerce électronique, sont, à notre estime, superflues. En effet, à l'analyse, on constate que, dans de nombreux cas, les contrats qui ressortissent à ces catégories ne peuvent être conclus par voie électronique dans la mesure où par ailleurs, les formes auxquelles ils sont soumis requièrent l'intervention des autorités publiques ou de professions exerçant une autorité publique (art. XII.16, 2°).

[33] En ce sens, voy. Ch. BIQUET-MATHIEU et S. NOTARNICOLA, « La protection des sûretés personnelles dites faibles – Le point après la loi du 3 juin 2007 sur le cautionnement à titre gratuit », *Sûreté et procédures collectives*, Liège, Anthemis, 2008, p. 56, n° 36 ; M. VANMEENEN, « Kosteloze borgtocht : (een) nieuwe zekerheid (?) », *R.D.C.*, 2008, p. 849, n° 10.

[34] Au cours des travaux préparatoires de la loi, une des parlementaires « plaide pour qu'on ne verse pas dans la surréglementation afin de ne pas rendre le cautionnement inattractif, en tant qu'élément de la vie économique. Ainsi, le projet de loi prévoit la formalité de la mention manuscrite, ce qui empêche les cautionnements électroniques, souvent utilisés dans le monde des affaires. Un formalisme exagéré implique le risque que d'autres moyens soient recherchés, précisément pour échapper à cette législation. En ce qui concerne la mention manuscrite, l'intervenante craint malgré tout que ce système entrave la souplesse, pourtant nécessaire, du cautionnement dans le cadre de transactions commerciales. En France, pays qui a servi de modèle pour ce système, l'on constate en effet une tendance à débarrasser le cautionnement de son formalisme. Ainsi la caution ne devrait-elle plus inscrire que la somme qu'elle garantit » (Rapport fait au nom de la Commission de l'économie, de la politique scientifique, de l'éducation, des institutions scientifiques et culturelles nationales, des classes moyennes et de l'agriculture par M. K. T'SIJEN, *Doc. parl.*, Ch. repr., sess. ord. 2006-2007, n° 2730/003, p. 7). À nos yeux, il convient de faire la part des choses : en soi, la formalité doit être maintenue dans la mesure où elle contribue clairement à protéger la partie faible. Si le problème réside dans l'impossibilité d'accomplir le contrat par voie électronique, la solution ne doit pas être de supprimer la formalité mais de faire en sorte qu'elle puisse être accomplie dans l'environnement numérique, au moyen d'un procédé fonctionnellement équivalent (voy. H. JACQUEMIN, *Le formalisme contractuel. Mécanisme de protection de la partie faible*, Bruxelles, Larcier, 2010, n° 296).

Dans l'intervalle, le règlement eIDAS offrira davantage de sécurité que le cadre normatif actuellement en vigueur.

Pour l'écrit, il n'existe pas encore de clause de non-discrimination. Ce principe est heureusement consacré par le règlement eIDAS, applicable à partir du 1er juillet 2016. Plus précisément, ce règlement consacre le principe pour le « document électronique ». Aux termes de l'article 46 du règlement eIDAS, « l'effet juridique et la recevabilité d'un document électronique comme preuve en justice ne peuvent être refusés au seul motif que ce document se présente sous une forme électronique ». Concrètement, le magistrat saisi d'un litige éventuel ne pourrait écarter l'acte de cession de rémunération électronique ou refuser de lui reconnaître la moindre efficacité juridique au seul prétexte qu'il est électronique. En tant que tel, il doit en tout cas l'examiner. Pour l'assimiler à un support papier, il incombe à l'entreprise de crédit de définir les fonctions attendues de la formalité et démontrer ensuite que le procédé utilisé dans l'environnement numérique permet de les atteindre avec un niveau d'efficacité suffisant. Pour ce faire, on peut utilement se référer aux enseignements de la doctrine, qui considère que l'écrit doit remplir une fonction de lisibilité, de pérennité et, même si cette fonction est plus contestée, une fonction d'intégrité. La clause transversale particulière relative à l'écrit (art. XII.15, § 2, du CDE) n'est pas applicable mais, partant du postulat de rationalité du législateur, on peut normalement considérer que l' « écrit » doit remplir les mêmes fonctions, quelles que soient les hypothèses dans lesquelles la formalité doit être mise en œuvre. Aussi pourrait-on se référer, *mutatis mutandis*, aux fonctions listées dans cette disposition.

S'agissant de la signature électronique (et même si l'article XII.15 n'est pas applicable), la situation devrait rester similaire. On peut en effet se fonder sur la clause de non-discrimination de l'article 4, § 5, de la loi du 9 juillet 2001 ou de l'article 25, § 1er, du règlement eIDAS. Pour assimiler le procédé à une signature manuscrite, on peut se fonder sur l'article 4, § 4, de la loi du 9 juillet 2001 qui assimile la signature électronique qualifiée à la signature manuscrite ou sur l'article 25, § 2, du règlement eIDAS. Il est par contre plus délicat de se référer à l'article 1322, alinéa 2, du Code civil, dès lors que de nombreux auteurs recommandent de limiter son application au droit de la preuve[35], plus précisément à la signature des actes sous

[35] On peut se fonder sur la place qu'il occupe dans le Code civil (l'art. 1322 est en effet inséré dans le livre III, titre III, chapitre VI, intitulé « De la preuve des obligations et de celle du paiement ») et sur le contexte d'adoption de la loi (voy. spéc. l'avis du Conseil d'État, *Doc. parl.*, Ch. repr., sess ord. 1998-1999 (lég. 49), n° 2141/001, p. 27, et l'introduction de l'expression « pour l'application du présent article »). En ce sens, voy. M. DEMOULIN et E. MONTERO, « Le formalisme contractuel à l'heure du commerce électronique », *Commerce électronique : de la théorie à la pratique*, Cahier du CRID n° 23, Bruxelles, Bruylant, 2003,

seing privé, requise conformément à l'article 1341 du même Code. Or, comme on l'a vu, les exigences de l'article 27 de la loi du 12 avril 1965 sont requises *ad validitatem*. On peut toutefois se référer aux définitions de la « signature électronique » et de la « signature électronique avancée », telles qu'elles figurent à l'article 2 de la loi du 9 juillet 2001[36], et aux fonctions qui s'en dégagent. En effet, la loi du 9 juillet 2001 ne limite pas son application aux formalités probatoires[37][38]. Dès l'application du règlement eIDAS (et l'abrogation corrélative de la loi du 9 juillet 2001), un tel raisonnement paraît plus contestable, en tout cas pour la signature électronique simple, puisque le règlement – à la différence de la loi du 9 juillet 2001 – n'énumère plus les fonctions attendues du procédé. Il indique plus largement qu'il s'agit des « données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique, et que le signataire utilise pour signer »[39]. Il faut donc rechercher en droit belge la signification généralement donnée à la signature ; or, des discussions ne manqueront pas de voir le jour suivant que l'on se fonde sur les fonctions reconnues par la doctrine et la jurisprudence à la signature manuscrite (authentification de l'origine et adhésion au contenu de l'acte) ou que l'on applique l'article 1322, alinéa 2, du Code civil, qui exige également du procédé qu'il maintienne l'intégrité du contenu de l'acte[40].

p. 184 (la « réforme n'affecte pas, en principe, les situations où une signature manuscrite est requise pour la validité d'un acte juridique ou son opposabilité aux tiers ») ; P. Lecocq et B. Vanbrabant, « La preuve du contrat conclu par voie électronique », *Le commerce électronique : un nouveau mode de contracter*, *op. cit.*, p. 127, n° 116 ; J. Dumortier et S. Van den Eynde, « De juridische erkenning van de elektronische handtekening in België », *Computerr*, 2001, p. 188 ; L. Guinotte, « La signature électronique après les lois du 20 octobre 2000 et du 9 juillet 2001 », *J.T.*, 2002, p. 558.

[36] Pour une application, en jurisprudence, voy. Conseil contentieux étrangers, 19 novembre 2009, n° 34364 : la validité d'un procédé de signature électronique est ainsi analysée à l'aune de l'article 2, 1°, de la loi du 9 juillet 2001 (signature électronique simple).

[37] M. Demoulin et E. Montero, « Le formalisme contractuel à l'heure du commerce électronique », *op. cit.*, p. 186.

[38] La lettre des dispositions-clés de la loi, qui énoncent les principes d'assimilation (art. 4, § 4) et de non-discrimination (art. 4, § 5), pourrait cependant instiller le doute. Le principe d'assimilation est établi, aux termes de l'article 4, § 4, « sans préjudice des articles 1323 et suivants du Code civil [...] », relatifs à la contestation de signature et d'écriture, en matière probatoire essentiellement. Quant à l'article 4, § 5, il dispose qu' « une signature électronique ne peut être privée de son efficacité juridique et ne peut être *refusée comme preuve en justice* au seul motif [...] » (nous soulignons). Si le doute existe, il n'emporte toutefois pas notre conviction. Rien n'empêche de contester une signature conformément aux règles des articles 1323 et suivants du Code civil lorsque celle-ci n'est pas requise uniquement dans une perspective probatoire. Quant au refus de la signature comme preuve en justice, il peut être considéré comme une application particulière de l'inefficacité juridique, qui recouvre également d'autres sanctions (la nullité de l'acte juridique pour défaut de signature, par exemple). Considérant que, nonobstant la formulation de la loi, l'irrecevabilité est une hypothèse, parmi d'autres, de l'inefficacité juridique, voy. P. Lecocq et B. Vanbrabant, « La preuve du contrat conclu par voie électronique », *op. cit.*, pp. 109-111 ; L. Guinotte, « La signature électronique après les lois du 20 octobre 2000 et du 9 juillet 2001 », *op. cit.*, p. 559.

[39] Art. 3, 10°, du règlement eIDAS.

SECTION 2. – Conclusion d'un contrat d'assurance par voie électronique

15.- Formes entourant la conclusion du contrat d'assurance. L'article 64 de la loi du 4 avril 2014 relative aux assurances[41] impose l'établissement d'un écrit, signé[42] et revêtu de diverses mentions informatives, pour prouver le contrat d'assurance et ses modifications. Le cas échéant, l'article 1325 du Code civil doit également être observé[43] : aussi faut-il, toujours dans une perspective probatoire, établir autant d'originaux qu'il y a de parties ayant un intérêt distinct.

On constate qu'à la différence du contrat de crédit à la consommation, les formes entourant la conclusion du contrat d'assurance et susceptibles de poser des difficultés dans l'environnement numérique sont requises

[40] Sur ce point, voy. la contribution de H. Jacquemin, dans le présent ouvrage.

[41] Cette disposition reprend, à droit constant, l'ancien article 10 de la loi du 25 juin 1992 sur le contrat d'assurance terrestre. Aussi peut-on avoir égard aux analysées consacrées à l'application de cette disposition dans l'environnement numérique – ou, de manière générale, à la conclusion du contrat d'assurance en ligne. Voy. les références citées *infra*, note 45.

[42] Même si l'exigence n'est pas expressément mentionnée, on estime généralement que, comme en droit commun, l'écrit requis doit être revêtu de la signature de la partie contre laquelle il faut prouver (E. Vieujean, « Le contrat d'assurance aujourd'hui », *Questions de droit des assurances*, Liège, Éd. du Jeune Barreau, 1996, p. 196 ; K. Troch et Ph. Colle, « Verzekeringen & Internet : Living apart together ? », *Mélanges offerts à Marcel Fontaine*, Bruxelles, Larcier, 2003, p. 646, n° 17 ; Ch.-A. Van Oldeneel, « Contrats électroniques d'assurance », *E-Business en assurance*, Dossier du *Bull. ass.* n° 9, 2003, p. 107. En jurisprudence, voy. par ex. Bruxelles, 25 février 1988, *R.G.D.C.*, 1990, p. 132, note Ph. Colle ; Civ. Bruges, 22 novembre 1995, *T.A.V.W.*, 1997, p. 199 ; Gand, 5 février 2004, *Bull. ass.*, 2004, p. 687).

[43] Tel est le cas lorsqu'il s'agit de prouver contre le preneur et que le contrat est de nature civile dans son chef. Dans un arrêt du 20 janvier 1984, la Cour de cassation a rappelé que, conformément à l'article 25 de la loi du 11 juin 1874 (actuellement, l'article 64 de la loi du 4 avril 2014), le contrat d'assurance doit être prouvé par écrit. Elle précise néanmoins qu' « en raison de l'article 25 du Code de commerce, l'article 1325 du Code civil n'est pas applicable et [...] plusieurs originaux ne devaient pas être rédigés » (Cass., 20 janvier 1984, *Pas.*, 1984, I, p. 552).

dans une perspective probatoire[44]. L'hypothèse se distingue donc de celle décrite précédemment concernant le contrat de crédit à la consommation. On observe également que le législateur n'est pas intervenu spécifiquement pour introduire des termes spécialement adaptés à l'environnement numérique ou désigner une forme particulière de signature électronique.

Partant du postulat que le secteur souhaite aller vers davantage de dématérialisation, pour conclure le contrat d'assurance en tant que tel, ou accomplir diverses formalités requises lors de la phase précontractuelle ou en cours d'exécution du contrat, la question se pose de savoir comment accomplir valablement les exigences requises dans l'environnement numérique[45]. A cet égard, comme on le verra, le règlement eIDAS apporte diverses solutions, en complément au cadre normatif existant.

16.- Application du règlement eIDAS pour lever les obstacles formels. Dès le 1er juillet 2016, le règlement eIDAS, en lien avec les dispositions pertinentes de la législation belge, sera applicable pour encadrer l'accomplissement des formes précitées dans l'environnement numérique.

Le procédé utilisé pour l'écrit – un document pdf, par exemple – et la signature – une signature électronique créée par la carte d'identité électronique, par exemple, ou un autre procédé de signature électronique – bénéficient du principe de non-discrimination[46]. Sur le plan probatoire, cela signifie qu'en cas de contestation[47], les procédés sont recevables et

[44] Sans doute peut-on le regretter, eu égard aux finalités poursuivies et à l'objectif de protection du preneur. Il n'en reste pas moins que la loi est très claire à ce sujet.

[45] Sur la conclusion du contrat d'assurance par voie électronique ou l'accomplissement de certaines exigences formelles, voy. not. K. Troch et Ph. Colle, « Verzekeringen & Internet : Living apart together ? », *op. cit.*, pp. 633 et s. ; Ch.-A. Van Oldeneel, « Contrats électroniques d'assurance », *E-Business en assurance*, Dossier du *Bull. ass.* n° 9, 2003, pp. 85 et s. ; M. Fontaine, *Droit des assurances*, 4e éd., Bruxelles, Larcier, 2010, pp. 145 et s., nos 195 et s. ; H. Jacquemin, « Conclusion et preuve du contrat d'assurance dans l'environnement numérique », *Forum de l'assurance*, 2010, n° 100, *La preuve en assurance*, pp. 249-255 ; Ph. Colle, *Algemene beginselen van het Belgische verzekeringsrecht*, 5e éd., Anvers, Intersentia, 2011 pp. 41-43, n° 43 ; H. Jacquemin, « Le formalisme du contrat d'assurance : analyse des règles en vigueur à l'aune des progrès techniques et de certaines pratiques contractuelles », La loi sur le contrat d'assurance terrestre, Bruxelles, Bruylant, 2012, pp. 43 et s. ; J. Dumortier, « Elektronische handtekening : juridische en praktische aspecten », *Assurances et technologies de l'information et de la communication, Bull. ass.*, dossier 2013, n° 19, pp. 85 et s. ; P. Van Eecke, « Nieuwe wetgeving vetrouwdiensten in de maak », *Bull. ass.*, dossier 2013, n° 19, pp. 113 et s. ; H. Jacquemin, « La conclusion du contrat d'assurance par voie électronique », *Bull. ass.*, dossier 2013, n° 19, pp. 37 et s.

[46] Art. 25 du règlement eIDAS pour la signature et art. 46 pour l'écrit, qui constitue un document électronique.

[47] Si la signature électronique n'est pas contestée, le juge doit lui reconnaître des effets juridiques identiques à ceux de la signature manuscrite.

doivent par conséquent faire l'objet d'un examen de la part de la juridiction compétente.

Dans un second temps, pour assimiler le procédé utilisé à un écrit signé, fonctionnellement équivalent et qui aura les mêmes effets en droit, il faut raisonner formalité par formalité. Concernant la signature, il peut s'agir soit d'une signature électronique qualifiée, au sens de l'article 3.12 du règlement eIDAS, soit d'une signature électronique au sens de l'article 1322, alinéa 2, du Code civil. Pour l'écrit, on doit avoir égard aux qualités fonctionnelles retenues à l'article XII.15, § 2, 1er tiret.

Concrètement, à défaut de signature électronique qualifiée (telle que la signature de la carte d'identité électronique), eu égard aux conditions de l'article 1322, alinéa 2, du Code civil, un juge pourrait être amené à accepter d'autres formes de signature électronique, exerçant ainsi le pouvoir d'appréciation que la loi lui octroie[48]. L'utilisation de logiciels de signature électronique, fondés sur la cryptographie asymétrique et téléchargeables sur l'internet pourrait suffire. Les procédés d'authentification utilisés dans le cadre de l'*internet banking* (le système du *digipass* associé à une carte bancaire, par exemple) pourraient également permettre de signer valablement, pour autant qu'ils garantissent également la fonction – certes contestable – de maintien de l'intégrité du contenu.

On pourrait également se demander si un contrat au format papier signé à la main par le preneur, puis scanné avant d'être envoyé par courrier électronique à la compagnie d'assurance (en pièce jointe) est muni d'une signature valable au sens de l'article 64 de la loi du 4 avril 2014. En admettant que l'*instrumentum* est muni d'une signature électronique, plus précisément d'une signature électronique simple[49], il convient d'appliquer le principe de non-discrimination et, dès lors, de se référer à l'article 1322, alinéa 2, du Code civil. En cas de contestation, le juge saisi du litige pourrait considérer que les conditions de cette disposition sont réunies lorsque, par exemple, le courriel du preneur est lui-même

[48] Enumérant des procédés *a priori* concernés par l'art. 1322, al. 2, C. civ., voy. E. Montero, « Introduction de la signature électronique dans le Code civil : jusqu'au bout de la logique 'fonctionnaliste' ? », *op. cit.*, pp. 196-197, n° 12 ; P. Lecocq et B. Vanbrabant, « La preuve du contrat conclu par voie électronique », *op. cit.*, pp. 117-118.

[49] Voy. en ce sens un arrêt n° 34.364 du Conseil du contentieux des étrangers, datant du 19 novembre 2009. Le Conseil se prononce sur la validité d'une signature scannée ou, plus précisément, de l'image au format électronique qui en résulte, et qui a été apposée sur un document électronique. Le procédé est considéré comme une signature électronique « ordinaire » au sens de l'article 2, 1°, de la loi du 9 juillet 2001 (points 3.12 et s. de l'arrêt). A ce propos, voy. E. Montero, « La signature électronique au banc de la jurisprudence », *DAOR*, 2011/98, pp. 233 et s. ; G. Vandendriessche, « An overview of some recent case law in Belgium in relation to electronic signatures », *Digital Evidence and Electronic Law Review*, 2010/7, pp. 90-100.

signé électroniquement (garantissant ainsi l'authenticité de l'origine et l'adhésion au contenu) et que, par ailleurs, l'intégrité du document n'est pas contestée. Par contre, si le contrat émane d'une adresse de courrier électronique plus fantaisiste (de type spiderman1243@gmail.com), le juge pourrait se montrer réticent à admettre que les fonctions d'authenticité de l'origine et d'adhésion ont été satisfaites : avec les outils multimédias actuels, il est en effet très facile de copier la signature manuscrite d'un tiers d'un document vers un autre, pour ensuite imprimer ce document, le scanner et l'envoyer par courriel depuis une adresse créée spécialement pour l'occasion.

17.- Recours aux autres services de confiance visés par le règlement eIDAS. Plusieurs dispositions de la loi du 4 avril 2014 relative aux assurances imposent des exigences particulières au moment de procéder à la transmission d'informations. La lettre recommandée (ou l'envoi recommandé) est ainsi prévue pour la résiliation du contrat d'assurance[50] ou pour la sommation envoyée en cas de défaut de paiement de la prime à l'échéance[51]. Aussi pourra-t-on se référer utilement aux dispositions du règlement en matière de service d'envoi recommandé électronique[52].

On sait par ailleurs que le contrat d'assurance se forme généralement par étapes, marquées par l'échange de l'un des documents visés à l'article 57 de la loi du 4 avril 2014 : la proposition d'assurance, la police présignée ou la demande d'assurance. Ces documents sont soumis à des conditions de forme spécifiques : ils doivent être établis par écrit, signés et revêtir certaines mentions. Aux termes de l'article 57, § 7, de la loi du 4 avril 2014, ces trois documents doivent également être datés par l'assureur, dès leur réception, pour éviter les abus et « accroître la sécurité juridique à l'occasion d'un processus où la chronologie revêt une grande importance »[53]. En effet, plusieurs délais prennent cours à la réception des documents. De même, pour le contrat d'assurance à distance, l'article 57, § 5, de la loi du 4 avril 2014 fixe la conclusion du contrat au moment où l'assureur reçoit l'acceptation du preneur. Il importe de déterminer ce moment avec précision, puisqu'il marque normalement le point de départ du droit de résiliation. Dans le cadre d'une procédure dématérialisée, la compagnie d'assurance pourra utiliser les services d'horodatage électronique tels que régis par le règlement eIDAS[54].

[50] Voy. l'article 18, § 1er, l'article 84, l'article 86 et l'article 100 de la loi du 4 avril 2014.
[51] Art. 70 de la loi du 4 avril 2014.
[52] Sur ce point, voy. la contribution de Ch. Verdure, dans le présent ouvrage.
[53] M. FONTAINE, *Droit des assurances*, Bruxelles, Larcier, 2010, p. 144, n° 192.
[54] Sur ce point, voy. la contribution de Ch. Verdure, dans le présent ouvrage.

CHAPITRE II. Perspectives ouvertes par le règlement eIDAS pour l'accomplissement d'opérations ponctuelles

18.- Le point dans trois hypothèses. Dans le domaine financier, l'encadrement de l'identification électronique et des services de confiance, tel que réalisé par le règlement eIDAS, constitue un outil particulièrement utile, ouvrant des perspectives intéressantes dans de nombreuses opérations ponctuelles. Nous les examinons dans le domaine des paiements sur l'identification à distance dans le cadre d'électroniques (section 1), avant de faire un focus sur la dématérialisation du mandat SEPA (Section 2) et la lutte contre le blanchiment (Section 3).

SECTION 1. – En matière de paiement électronique

§ 1. Partage de responsabilité en cas d'opérations de paiement non-autorisées

19.- Partage de responsabilité. L'article VII.36 du Code de droit économique règle le partage de responsabilités entre le payeur et le prestataire de services de paiements (banque, établissement de paiement, établissement de monnaie électronique, etc.) en cas d'opération de paiement non autorisées[55].

En l'absence de fraude, d'intention ou de négligence grave, la responsabilité du payeur est plafonnée, avant la notification, à 150 EUR pour « les pertes liées à toute opération de paiement non autorisée consécutive à l'utilisation d'un instrument de paiement perdu ou volé ou, si le payeur n'est pas parvenu à préserver la sécurité de ses dispositifs de sécurité personnalisés, au détournement d'un instrument de paiement »[56].

[55] Pour un commentaire du régime établi par la loi du 10 décembre 2009 sur les services de paiement, désormais abrogée et remplacée par le livre VII du CDE, voy. J. FELD, « Le paiement électronique à la lumière de la nouvelle loi sur les services de paiement », *Le paiement*, Louvain-la-Neuve, Anthemis, 2009, pp. 63 et s. ; R. STEENNOT, « Girale en elektronische betalingen », *NjW*, 2010, pp. 518 et s. ; R. STEENNOT et T. BAES, « Wet op belatingsdiensten : bescherming of overbescherming ? », *B.F.R.*, 2010, pp. 208 et s. ; H. JACQUEMIN, « Les paiements électroniques dans les contrats à distance depuis la loi du 10 décembre 2009 », *R.D.T.I.*, 2010/41, pp. 10 et s. ; C. ALTER, « Le paiement électronique », *Incidence des nouvelles technologies de la communication sur le droit commun des obligations*, Bruxelles, Bruylant, 2012, pp. 95 et s.
[56] Art. VII.36, § 1er, al. 1, du CDE. L'objectif est d'inciter l'utilisateur à notifier la perte ou le vol dans les meilleurs délais.

20.- Moyen de paiement utilisé sans présentation physique et sans identification électronique. Sauf en cas de fraude ou de manquement intentionnel, par le payeur, aux obligations prescrites par l'article VII.30 du Code de droit économique, une exception est toutefois introduite par la loi en vue de dispenser celui-ci de toute perte occasionnée par une opération de paiement non autorisée. Tel est le cas « si l'instrument de paiement a été utilisé sans présentation physique et sans identification électronique » (art. VII.36, § 1er, al. 3, 1°, du CDE). Cette exception pourra généralement être invoquée en matière de contrats à distance puisque, par définition, la conclusion de ceux-ci doit se faire sans la présence physique et simultanée des parties (par téléphone ou à travers un site internet, par exemple)[57].

Reste à comprendre la notion « d'identification électronique ». Les travaux préparatoires de la loi du 10 décembre 2009, désormais intégrée dans le livre VII du Code, nous enseignent que « l'identification électronique vise le cas où l'instrument est par exemple identifié au moyen d'un lecteur de carte ('smart cart reader')[58]. Avant l'entrée en vigueur de la loi du 10 décembre 2009, cette question était régie par l'article 8 de la loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds[59], qui prévoyait une règle similaire. Les travaux préparatoires relatifs à cette disposition évoquaient le recours à un mécanisme de signature électronique[60]. En pratique, les banques proposent des lecteurs de carte ou des *digipass* qui génèrent un code chiffré nécessaire pour accéder au service en ligne et effectuer des transactions. *A priori*, ces mécanismes permettent à tout le moins d'authentifier l'identité du titulaire et, par conséquent, remplissent la condition relative à l'identification électronique, au sens de la loi[61].

[57] L'objectif du législateur est clair : encourager les prestataires de services de paiement à mettre en place des dispositifs suffisamment sécurisés lorsque les parties ne sont pas en présence physique l'une de l'autre lors du paiement (hypothèses dans lesquelles les risques de fraudes sont plus importants).

[58] Commentaire des articles du projet de loi relatif aux services de paiement, *Doc. parl.*, Ch. repr., sess ord. 2008-2009, n° 2179/001, p. 71. Il est intéressant de noter que la disposition correspondante du projet de loi était complétée comme suit : « le simple usage d'un code confidentiel ou d'une autre preuve similaire de l'identité n'est pas suffisant pour engager la responsabilité du payeur » (*Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/001, p. 131). Cette formule a toutefois disparu dans les versions ultérieures, sans véritable explication. Il ne semble toutefois pas que la volonté ait été d'aller à l'encontre de cette considération, à la lumière du commentaire de l'article tiré des travaux préparatoires.

[59] *M.B.*, 17 août 2002. Sur cette disposition, voy. not. M. Demoulin, « Le paiement électronique », *Obligations. Traité théorique et pratique*, Bruxelles, Kluwer, 2007, V.1.7, p. 26 ; Th. Lambert, « La loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds », *R.D.C.*, 2003, p. 584, n° 40 ; O. Goffard, « 'Status quaestionis' : risques et responsabilités en cas de transfert électronique de fonds », *R.D.C.*, 2005, pp. 5 et s.

[60] *Doc. parl.*, Ch. repr., sess. ord. 2000-2001, n° 1389/001, p. 36. Il n'est plus fait expressément référence à un procédé de signature électronique dans les travaux préparatoires de la loi du 10 décembre 2009 mais celui-ci constitue assurément l'un des moyens auxquels les prestataires peuvent recourir pour atteindre les fonctions attendues.

21.- Évolutions dans la DSP 2. Des modifications sont apportées en la matière par la DSP 2[62], en particulier à l'article 74 de la directive. Parmi les principales, on note la réduction du montant maximal que l'utilisateur doit supporter (qui passe de 150 à 50 euros) et une possible responsabilité du prestataire de service du payeur ou du bénéficiaire (ou de son prestataire de service de paiement) lorsqu'une authentification forte du client n'est pas exigée ou acceptée.

§ 2. Exigences d'authentification forte prévue par la DSP 2

22.- DSP 1 et DSP 2. La deuxième version de la Directive sur les Services de Paiement (DSP 2)[63] a été adoptée le 25 novembre 2015. Elle abroge et remplace la première Directive sur les Services de Paiement (DSP 1) du 13 novembre 2007[64].

Entrée en vigueur le 13 janvier 2016, les États membres disposent d'un délai de deux ans pour la transposer. Les nouvelles dispositions seront donc applicables à compter du 13 janvier 2018.

23.- La question de l'authentification prend de plus en plus d'ampleur dans le cadre de la sécurisation des transactions. Réaffirmant que « la sécurité des paiements électroniques est fondamentale pour garantir la protection des utilisateurs et le développement d'un environnement sain pour le commerce électronique », la DSP 2 dispose, en son consi-

[61] Du reste, les conditions contractuelles établies par les institutions bancaires (et auxquelles le client consent en ouvrant un compte et en utilisant les services qui y sont associés) contiennent généralement des dispositions relatives à la preuve de certaines opérations, notamment les paiements réalisés au moyen de l'informatique et des technologies de l'information.

[62] Voy. les réf. citées à la note suivante.

[63] Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE, *J.O.*, L. 337 du 23 décembre 2015.

[64] Directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE, *J.O.*, L. 319 du 5 décembre 2007.

dérant n° 95, que « tous les services de paiement proposés par voie électronique devraient être sécurisés, grâce à des technologies permettant de garantir une authentification sûre de l'utilisateur et de réduire, dans toute la mesure du possible, les risques de fraude ». La directive consacre dès lors un chapitre complet aux risques opérationnels, à la sécurité et à l'authentification.

En ce sens, il existe des liens étroits avec l'identification électronique et certains services de confiance, en particulier les services de signature électronique (tels que visés par le règlement eIDAS).

24.- Les nouveaux services d'initiation d'ordre de paiement et d'information sur les comptes. Cette question est cruciale eu égard au développement de nouveaux services, et notamment des services techniques qui ont recours à l'utilisation des procédures d'authentification du client pour accéder à son compte.

Deux de ces services techniques – le service d'initiation d'ordre de paiement et le service d'information sur les comptes – sont d'ailleurs devenus de vrais services de paiement avec la DSP 2, basculant de la sphère libre à la sphère régulatoire en raison des enjeux de sécurité et de responsabilité qu'ils engendraient. Aussi leur exercice sera-t-il dorénavant soumis à un agrément préalable.

Le service d'initiation d'ordre de paiement consiste en la mise en place d'une passerelle logicielle entre un site internet d'e-commerce et la plateforme de banque en ligne de l'établissement gestionnaire du compte du payeur pour initier des paiements par internet sur la base d'un virement[65].

Le service d'information sur les comptes permet à un utilisateur d'avoir accès aux informations relatives à un ou plusieurs de ses comptes détenus auprès d'un ou de plusieurs établissements, de manière agrégée, ce qui permet à l'utilisateur d'avoir immédiatement une vue d'ensemble de sa situation financière à un moment donné[66].

Les prestataires de service d'initiation d'ordre de paiement ou d'information sur les comptes, utilisent donc la procédure d'authentification du client pour accéder au compte disponible dans son *internet/mobile banking* traditionnel. En conséquence, dans la mesure où ces nouveaux services innovants entrent dans le champ de la régulation et sont fortement dépendants de l'accès au compte du client détenu dans un autre établissement, la directive a expressément prévu que les États membres devaient veiller à ce que ces prestataires puissent se fonder sur les procédures

[65] Voy. la définition figurant à l'article 4, 15°, de la DSP 2.
[66] Voy. la définition figurant à l'article 4, 16°, de la DSP 2.

d'authentification prévues par l'établissement gestionnaire du compte à l'intention de son client[67].

25.- Le rôle de l'ABE dans la définition des normes techniques. Afin de garantir une application cohérente de la directive, la Commission européenne s'appuie sur l'expertise et le soutien de l'Autorité bancaire européenne (ABE), qui est chargée d'élaborer des orientations et des projets de normes techniques de réglementation relatives aux questions de sécurité en matière de services de paiement, en particulier pour ce qui concerne l'authentification forte du client, et sur la coopération entre les États membres dans le contexte de la prestation de services et de l'établissement dans d'autres États membres des établissements de paiement agréés[68].

L'article 98 de la DSP2 dispose que l'ABE, en étroite collaboration avec la BCE, est chargée d'élaborer des projets de normes techniques de réglementation à l'intention des prestataires de services de paiement précisant notamment :

a) les exigences relatives à l'authentification forte du client ;

b) les dérogations à l'application de l'authentification forte ;

c) les exigences auxquelles doivent satisfaire les mesures de sécurité, afin de protéger la confidentialité et l'intégrité des données de sécurité personnalisées de l'utilisateur de services de paiement ; et

d) « les exigences applicables aux normes ouvertes communes et sécurisées de communication aux fins de l'identification, de l'authentification, de la notification et de l'information, ainsi que pour la mise en œuvre des mesures de sécurité, entre les prestataires de services de paiement gestionnaires du compte, les prestataires de services d'initiation de paiement, les prestataires de services d'information sur les comptes, les payeurs, les bénéficiaires et d'autres prestataires de services de paiement ».

L'ABE devra définir des normes techniques permettant, conformément à l'article 98, de :

« a) garantir un niveau de sécurité approprié pour les utilisateurs de services de paiement et les prestataires de services de paiement par l'adoption d'exigences efficaces et fondées sur les risques ;
b) garantir la sécurité des fonds et des données à caractère personnel des utilisateurs de services de paiement ;
c) garantir et maintenir une concurrence équitable entre l'ensemble des prestataires de services de paiement ;

[67] Art. 97 de la DSP 2.
[68] Considérant n° 107 de la DSP 2.

d) garantir la neutralité du modèle commercial et des technologies ;
e) permettre le développement de moyens de paiement innovants, accessibles et faciles à utiliser ».

C'est donc sur la base de ce fondement légal que l'ABE a publié le 8 décembre 2015 un « Discussion Paper » relatif aux normes techniques « regulatory technical standards on strong customer authentication and secure communication under PSD2 »[69], l'objectif étant d'identifier et caractériser les problèmes que la future approche réglementaire aura pour but de modérer, et de demander aux répondants d'exprimer leur point de vue sur la façon dont l'ABE a identifié et caractérisé le problème. L'objectif majeur qui est poursuivi par l'ABE est la sécurité des paiements électroniques et la garantie de l'authentification du client afin de réduire au minimum le risque de fraudes. Le document contient une vingtaine de questions, réparties en cinq thématiques, qui rappellent l'article 98 de la DSP 2 :

- authentification forte du client ;
- dérogations à l'application de la procédure d'authentification forte ;
- protection de la confidentialité et de l'intégrité des données de sécurité de l'utilisateur de services de paiements ;
- exigences applicables aux normes ouvertes communes et sécurisées de communication ;
- possibles synergies avec le règlement eIDAS sur l'identification électronique.

Les acteurs du secteur étaient invités à répondre avant le 8 février 2016. Les réponses reçues sur le *discussion paper* serviront à alimenter la réflexion de l'ABE qui établira un premier projet de normes techniques divulgué durant l'été 2016, et soumis ensuite à consultation pendant une période de 3 mois.

Alors que la DSP2 devra être transposée en janvier 2018, les normes techniques y afférentes, ne devraient pas, quant à elles, entrer en vigueur avant octobre 2018.

26.- Notion d'authentification simple et d'authentification forte. La DSP 2 ne définit pas l'identification, mais le fait pour l'authentification « simple » et l'authentification « forte ». En fonction des données de sécurité personnalisées qui seront demandées lors de l'authentification et de leurs canaux de transmission, il pourra s'agir d'une authentification

[69] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2.

simple ou d'une authentification forte (utilisation de lecteur de carte, téléphone mobile, digipass, email, signature électronique qualifiée, etc.).

La directive définit les critères à satisfaire pour garantir une authentification (simple) de l'utilisateur. La procédure mise en place doit permettre au prestataire de services de paiement de « vérifier l'identité d'un utilisateur de services de paiement ou la validité de l'utilisation d'un instrument de paiement spécifique, y compris l'utilisation des données de sécurité personnalisées de l'utilisateur »[70] (c'est-à-dire des données fournies à un utilisateur par le prestataire de paiement pour accéder à son compte ou utiliser un moyen de paiement par exemple).

Pour procéder à une authentification forte au sens de DSP 2, il faut que la procédure d'authentification remplisse trois conditions cumulatives :

1. L'authentification doit reposer sur l'utilisation de deux éléments au moins appartenant aux catégories « connaissance » (quelque chose que seul l'utilisateur connaît – par exemple, un mot de passe fixe, un code, un numéro d'identification personnel), « possession » (quelque chose que seul l'utilisateur possède – par exemple un jeton ou « token », une carte à puce, un téléphone mobile) et « inhérence » (quelque chose que l'utilisateur est – par exemple une caractéristique biométrique, telle qu'une empreinte digitale ou une empreinte de l'iris).
2. Les éléments d'authentification doivent être indépendants, en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres.
3. La procédure d'authentification est conçue de manière à protéger la confidentialité des données d'authentification.

Le recours à une procédure d'authentification « forte » implique dès lors que la confidentialité des données transmises soit assurée et que la procédure repose sur la combinaison d'éléments de natures différentes et indépendantes l'une de l'autre afin que la compromission de l'un n'entraine pas la compromission de l'autre. Un des éléments utilisés doit être non réutilisable et non reproductible de sorte que si quelqu'un arrive à intercepter la combinaison d'informations transmises pour l'authentification, les données ne soient pas réutilisables.

27.- Nécessité de garantir la fiabilité de la procédure d'authentification. Les modalités de sécurisation mises en place devront assurer la confidentialité et l'intégrité des données de sécurité personnalisées utilisées pour l'authentification, d'autant plus que le titulaire du compte ou

[70] Art. 4, 29°, de la DSP 2.

payeur fait souvent l'objet de tentatives d'attaques de fraudeurs, pas nécessairement toujours très complexes, telles que l'envoi de messages emails d'hameçonnage (phishing) avec des liens qui redirigent l'internaute vers des sites frauduleux permettant de récupérer ses données d'identification. On songe aussi à la propagation de logiciels malveillants infectant les devices de l'utilisateur (ordinateur, tablette, téléphone mobile...) et permettant de capturer les frappes d'informations saisies par les utilisateurs.

S'agissant de la lutte contre le phishing, les certificats d'authentification de sites internet devraient apporter des éléments de solution. Ce certificat constituant une « attestation qui permet d'authentifier un site internet et associe celui-ci à la personne physique ou morale à laquelle le certificat est délivré ». Si le règlement eIDAS encadre ce nouveau service de confiance consistant à délivrer des certificats d'authentification de site internet, les règles applicables en la matière restent cependant très sommaires puisque le règlement eIDAS se limite à prévoir que « les certificats qualifiés d'authentification de site internet satisfont aux exigences fixées à l'annexe IV » (art. 45).

L'indépendance des éléments d'authentification pose également des questionnements lorsque l'utilisateur utilise une application pour accéder à son compte ou procéder à un paiement et que dans le même temps l'appareil (*device*) sur lequel l'application est exécutée sert à recevoir ou récupérer les informations d'identification (par exemple par SMS, email, accès au cloud) ou qu'il contient les informations d'identification (par exemple dans le cadre du matériel et/ou de la couche logicielle). Ce point fait d'ailleurs l'objet de réflexions au sein de l'Autorité bancaire européenne (ABE) qui a publié une note sur le projet à venir de règles techniques applicables à l'authentification forte du client mise en place par la DSP 2[71].

28.- Application de l'authentification forte. Avec la DSP 2, les prestataires de services de paiement auront désormais l'obligation d'appliquer des procédures d'authentification forte du client dans certaines situation précises jugées à risque et nécessitant le renforcement de la sécurisation de l'authentification.

Ainsi par application de l'article 97, l'authentification forte sera requise lorsque le payeur :

1. accède à son compte de paiement en ligne ;
2. initie une opération de paiement (paiements par carte, virements, transactions e-money, prélèvement automatique) ;

[71] https://www.eba.europa.eu/-/eba-seeks-input-on-strong-customer-authentication-and-secure-communication-under-psd2

3. exécute une action, via un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation frauduleuse. Cette troisième situation peut recouvrir différentes opérations, telles que les actions liées à l'activation et à la désactivation des fonctionnalités de paiement, le changement de la liste des bénéficiaires de virements, etc.

Dans le cadre de l'initiation d'opération de paiement électronique à distance, les prestataires de services de paiement devront de plus, dans le cadre de la procédure d'authentification forte mise en place, intégrer des éléments qui établissent un lien dynamique entre l'opération, le montant et le bénéficiaire donnés.

29.- Dérogations à l'obligation d'authentification forte par une appréciation des risques liés à l'opération envisagée. Le considérant n° 96 précise que, « afin de permettre le développement de moyens de paiement accessibles et faciles à utiliser pour les paiements présentant peu de risques, tels que les paiements de faible valeur sans contact au point de vente, qu'ils soient ou non fondés sur la téléphonie mobile, les dérogations à l'application des exigences de sécurité devraient être précisées dans les normes techniques de réglementation ». C'est donc l'ABE, en étroite coopération avec la BCE, qui devra, conformément aux termes de l'article 98, § 3, de la DSP 2, définir les dérogations aux obligations d'authentifications fortes sur base des critères suivants :

- le niveau de risque lié au service fourni ;
- le montant, le caractère récurrent de l'opération ou les deux ;
- le moyen utilisé pour exécuter l'opération.

Dans le cadre du *discussion paper*[72] publié en décembre, l'ABE rappelle que la DSP2 ne détaillant pas les critères applicables aux dérogations à l'obligation d'authentification forte, il conviendra de clarifier ces notions et propose quelques exemples de situations qui pourraient remplir les critères fixés par la DSP2 pour pouvoir déroger à l'obligation d'authentification forte :

- les paiements effectués avec des instruments de paiement de faible valeur[73] définis par la DSP2 dès lors que les risques sont surveillés ;

[72] https://www.eba.europa.eu/-/eba-seeks-input-on-strong-customer-authentication-and-secure-communication-under-psd2.

[73] Auxquels le considérant n° 81 fait référence et qui dispose que « les instruments de paiement relatifs à des montants de faible valeur devraient constituer un moyen simple et bon marché de régler des biens et des services de faible prix et ne devraient pas être soumis à des exigences excessives. Les exigences d'information et les règles relatives à l'exécution

- les paiements effectués à des bénéficiaires effectifs qui sont déjà connus de l'établissement (liste blanche) ;
- les transferts entre deux comptes appartenant au même utilisateur tenus au sein du même établissement ;
- les transactions représentant un faible-risque basées sur une analyse de risque de la transaction (en prenant en compte les critères détaillés dans les règles techniques) ;
- les services purement consultatifs, sans affichage de données de paiement sensibles[74], prenant en considération la réglementation relative à la protection des données à caractère personnel.

30.- L'ABE veut identifier les synergies entre la DSP 2 et l'identification électronique (eIDAS). Le règlement eIDAS fixe un certain nombre de règles relatives à l'identification électronique et aux services de confiance pour les transactions électroniques au sein du marché intérieur. Dans le cadre de l'élaboration des normes techniques, l'ABE considère que les questions traitées par le règlement pourraient offrir des solutions aux PSP afin de mettre en œuvre des procédures d'authentification forte des clients pour protéger la confidentialité et l'intégrité des données de sécurité personnalisées ou pour mettre en œuvre « les exigences applicables aux normes ouvertes communes et sécurisées de communication aux fins de l'identification, de l'authentification, de la notification et de l'information, ainsi que pour la mise en œuvre des mesures de sécurité, entre les prestataires de services de paiement gestionnaires du compte, les prestataires de services d'initiation de paiement, les prestataires de services d'information sur les comptes, les payeurs, les bénéficiaires et d'autres prestataires de services de paiement »[75].

Il faut effectivement plaider pour que, dans la mesure du possible, une cohérence soit assurée entre les deux instruments, de sorte que les utilisateurs puissent recouvrir aux procédés techniques mis à leur disposition pour le plus grande nombre possible de services.

qui leur sont applicables devraient donc être limitées aux informations essentielles, compte tenu également des capacités techniques que l'on est en droit d'attendre d'instruments spécialisés dans les paiements de faible valeur. Malgré ce régime allégé, les utilisateurs de services de paiement devraient bénéficier d'une protection adéquate étant donné les risques limités que présentent ces instruments de paiement, en particulier pour ce qui est des instruments de paiement prépayés ».

[74] Les données de paiement sensibles sont « des données, y compris les données de sécurité personnalisées, qui sont susceptibles d'être utilisées pour commettre une fraude. En ce qui concerne les activités des prestataires de services d'initiation de paiement et des prestataires de services d'information sur les comptes, le nom du titulaire du compte et le numéro de compte ne constituent pas des données de paiement sensibles ».

[75] https://www.eba.europa.eu/-/eba-seeks-input-on-strong-customer-authentication-and-secure-communication-under-psd2.

31.- Les prestataires de services de paiement sont responsables des mesures de sécurité mises en place. Il leur appartient donc de mettre en place une procédure adéquate de surveillance, de traitement et de suivi des incidents de sécurité et des réclamations de clients liées à la sécurité, y compris un mécanisme de signalement des incidents. Les mesures de sécurité mises en place doivent être proportionnées aux risques de sécurité concernés et maintenues à jour. L'article 96 de la DSP 2 met d'ailleurs à la charge des prestataires de services de paiement des obligations de notification des incidents opérationnel ou de sécurité majeur. L'établissement doit sans retard injustifié, informer l'autorité compétente de l'État dans lequel il est établit ainsi que ses clients lorsqu'il existe un risque de répercussions sur les intérêts financiers des utilisateurs de services de paiement. Les prestataires de services de paiement devront fournir à leurs autorités compétentes, au moins chaque année, des données statistiques relatives à la fraude liée aux différents moyens de paiement. D'ici au 13 janvier 2018, l'ABE, en étroite coopération avec la BCE et après avoir consulté toutes les parties concernées devra émettre des orientations de mises en œuvre de ces dispositions.

Avec le renforcement des obligations de sécurité, qui ne se limitent pas aux données personnelles, le recours aux procédures de signatures électroniques et de cachets électroniques harmonisés au niveau européen font dès lors partie de l'arsenal à disposition des établissements financiers pour sécuriser tant techniquement que juridiquement les systèmes d'informations bancaires et les interactions avec les clients et les autres prestataires de services de paiement et partenaires techniques.

SECTION 2. – Dématérialisation du prélèvement électronique SEPA (SDD Care)

32.- Dispositions en matière de domiciliation. Le Code de droit économique définit la domiciliation comme suit : « service de paiement visant à débiter le compte de paiement d'un payeur, lorsqu'une opération de paiement est initiée par le bénéficiaire sur la base du consentement donné par le payeur au bénéficiaire, au prestataire de services de paiement du bénéficiaire ou au propre prestataire de services de paiement du payeur » (art. I.9.13°, CDE).

L'article VII.28, § 1er, du Code de droit économique précise les conditions dans lesquelles doit être réalisée une domiciliation :

« La réalisation de la domiciliation nécessite l'*octroi d'un mandat* par le payeur à, selon le cas, l'une ou plusieurs des personnes suivantes :
1° le bénéficiaire ; 2° le prestataire de services de paiement du bénéficiaire ; 3° le prestataire de services de paiement du payeur. Un exemplaire doit être remis au payeur.
§ 2. Même si le mandat visé au § 1er, alinéa 1er, n'est pas repris dans le même *instrumentum* que le contrat principal dont il garantit l'exécution, le mandat répond au moins aux conditions suivantes :
1° un *consentement exprès* du payeur ;
2° la procuration à donner doit se référer expressément au contrat sous-jacent qui a son tour détermine la portée des créances domiciliées en ce qui concerne la nature, l'échéance et, si possible, le montant juste. La domiciliation ne peut se réaliser valablement que si le payeur a été précédemment informé du contrat sous-jacent.
§ 3. Sans préjudice de l'application de l'article VII. 37, § 3, si le montant juste ou la date de débit n'est pas déterminée lors de la conclusion de la domiciliation, le bénéficiaire en fait part au payeur à la date convenue, dans un délai raisonnable précédant l'initiation de chaque opération de paiement.
§ 4. Une domiciliation et le mandat y attaché peuvent être résiliés par chaque partie, à tout moment, par la notification au cocontractant.
La résiliation de la domiciliation par le payeur est valable et opposable à tous ses mandataires lorsque le payeur la notifie soit à son créancier, soit à son prestataire de services de paiement si cette dernière possibilité a été expressément convenue »[76].

La mise en œuvre d'un mandant nécessite donc que le consentement exprès du payeur soit recueilli, lorsque ce mandat est électronique, il pourra être effectué au moyen de l'apposition d'une signature électronique.

33.- Les règles européennes relatives au prélèvement électronique SEPA. Ces règles se trouvent dans diverses dispositions normatives ou techniques adoptées au niveau européen. On retient notamment le règlement (UE) n° 260/2012 du Parlement européen et du Conseil du 14 mars 2012 établissant des exigences techniques et commerciales pour les virements et les prélèvements en euros et modifiant le règlement (CE) n° 924/2009 et le *SEPA Core Direct Debit Scheme Rulebook* publié par le Conseil européen des paiements (European Payment Council – EPC).

[76] Nous soulignons.

Le mandat de prélèvement SEPA doit obligatoirement contenir diverses mentions (coordonnées du créancier ; identifiant Créancier SEPA (ICS) ; référence unique du Mandat (RUM) ; coordonnées du payeur et références bancaires du payeur (BIC/IBAN)).

Le mandat signé doit ensuite être remis ou adressé au créancier, la conservation de celui-ci, sous forme papier ou électronique, étant de sa responsabilité.

34.- Exigence d'une signature qualifiée pour le E-mandate de l'EPC ? En vertu du SEPA Core Direct debit Schemes rulebook[77], publié par l'European Payments Council (ci-après l' « EPC »), la signature du mandat électronique doit être effectuée par signature qualifiée : « *The paper mandate can be stored either as the original document or in any digitalised format subject to the national legal requirements. Alternatively, the Mandate may be an electronic document which is created and signed with a Qualified Electronic Signature agreed between the Creditor and the Creditor Bank.*

[...]

When electronic, the data elements must be extracted from the electronic document without altering the content of the electronic Mandates ».

De plus, pour émettre le eMandate défini par l'EPC, le payeur doit utiliser un canal électronique proposé par le bénéficiaire pour compléter ledit mandat avec les données requises, d'une part, s'identifier et s'authentifier conformément aux instructions reçues de la part de son prestataire de services de paiement, et selon les moyens d'authentification mis en place par lui, d'autre part.

La procédure d'authentification prévue en l'espèce impliquait donc que, pour consentir un mandat de domiciliation électronique, le payeur s'identifie et s'authentifie selon la procédure définie avec sa banque (à l'image de ce qui est appliqué dans le cadre d'un paiement par carte bancaire, lorsque l'authentification 3DSecure est mise en place). Les procédures techniques devaient être compatibles techniquement avec l'EPC e-Operating Model for e-Mandates[78], ce qui était très contraignant, car elles impliquaient le concours de tous les établissements financiers et l'adoption d'une procédure harmonisée d'authentification fondée sur

[77] http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/sepa-direct-debit-core-rulebook-version-70/epc016-06-core-sdd-rb-v71-approvedpdf/.

[78] http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/epc-e-mandates-e-operating-model-high-level-definition/epc109-08-e-mandates-e-operating-model-high-level-definitionv1-5-approvedpdf/.

l'intervention de la banque du payeur. Aussi le e-mandate défini par l'EPC ne s'est-il jamais déployé.

Dès 2013, l'EPC et la Commission européenne[79] ont toutefois relativisé les exigences de signature qualifiée. En effet, ils ont précisé que la solution E-mandate définie par l'EPC n'était pas exclusive d'autres solutions de mandats électroniques. Selon l'EPC, en effet : « *we hereby wish to clarify that the signature methods as described in Section 4.1 of the SDD Scheme Rulebooks are not exhaustive and that SDD Scheme Participants may consider allowing continued usage of other legally binding methods of signature including those that were used under the local legacy scheme rules until now provided that they comply with the SEPA Regulation*"[80]. Le 16 avril 2015, l'EPC réaffirme sa position[81] qui sera finalement entérinée dans la version du 22 novembre 2015 des *SDD core Rulebook 8.1*. Le mandat SEPA peut être un document électronique signé en utilisant une méthode de signature juridiquement engageante. En conséquence, l'exigence d'une signature électronique qualifiée est supprimée.

L'interprétation des conditions à satisfaire pour la signature avancée a conduit à exclure dans un premier temps les signatures serveurs, créant une insécurité juridique. Bien que le Forum of European Supervisory Authorities for Electronic Signatures (FESA) ait considéré à plusieurs reprises que la condition visant à ce que la signature électronique soit créée par des moyens que le signataire puisse garder sous son contrôle exclusif n'impliquait pas l'utilisation d'un matériel dédié à la création de la signature électronique mettant ainsi en évidence le principe de neutralité des technologies utilisées pour créer une signature électronique[82], il régnait sur ce sujet une grande incertitude constituant un frein à la dématérialisation des mandats SEPA. Selon Stephen Mason[83], « la signification de l'expression « créée par des moyens que le signataire peut garder sous son contrôle exclusif » n'est pas claire » et « pourrait signifier garder la possession matérielle des moyens, ou ne pas divulguer les informations d'authentification ». En d'autres termes, selon la doctrine, l'ambiguïté de cette condition pouvait renvoyer à deux acceptions aux conséquences

[79] http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2013-009922&language=EN.

[80] EPC Clarification Letter on Electronic Mandates to SEPA Direct Debit Scheme Participants, 2.10.13, http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/clarification-letter-on-electronic-mandates-to-sepa-direct-debit-scheme-participants/letter-epc098-13-clarification-letter-to-sdd-scheme-participantspdf.

[81] EPC Clarification Paper on the Use of Electronic Mandate Solutions.

[82] Voy. : FESA, *Working paper on advanced electronic signature*, 12 octobre 2004 et FESA, *Public Statement on server based signature services*, 17 octobre 2005.

[83] S. Mason, *Electronic Signatures in Law*, 3e éd., Cambridge, 2012, p. 121.

pratiques bien différentes. Dans un cas, il est possible d'imaginer que le signataire gardera sous son contrôle exclusif les moyens de signature dès lors qu'il a en sa possession le matériel nécessaire pour générer cette signature. Dans l'autre, il est possible d'imaginer que même si le signataire n'a pas en sa possession le matériel nécessaire pour générer la signature, le fait que les informations d'identification restent secrètes permet de satisfaire à la condition susvisée.

Avec le règlement eIDAS, c'est un corpus plus adapté qui entre en vigueur. Précisons, concernant spécifiquement la signature serveur, que c'est finalement l'interprétation la plus favorable qui a été retenue puisque le nouveau texte ne conditionne plus la qualification de signature électronique avancée au fait que le signataire puisse « garder sous son contrôle exclusif les moyens ayant permis la création de la signature » mais au fait que la signature soit créée à l'aide de « données de création de signature que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif »[84].

SECTION 3. – Lutte contre le blanchiment de capitaux et obligation d'identification des clients

35.- Obligation de vérification de l'identité. Quid à distance ? Les prestataires de services de paiement ont l'obligation, lorsqu'ils nouent une relation d'affaire, de s'informer sur le client, ce qui exige notamment de vérifier son identité sur la base de documents probants.

Lorsque cette vérification s'effectue sans présence physique du client, la situation devient plus se complexe : de l'envoi de documents scannés à la lecture de carte d'identité électronique, en passant par l'utilisation de webcams, force est de constater que les modalités et la fiabilité de ces vérifications fluctuent fortement d'un procédé ou d'un pays à un autre.

Ainsi, en Belgique, l'article 7, § 2, du règlement de la Commission bancaire, financière et des assurances du 27 juillet 2004 relatif à la prévention du blanchiment de capitaux et du financement du terrorisme, prévoit que lorsque l'identification des clients personnes physiques est effectuée à distance, la vérification de leur identité doit être opérée :

1° au moyen de la carte d'identité électronique du client (eID) ;

[84] Voy. la définition figurant à l'article 3, 11°, et le renvoi aux conditions de l'article 26 du règlement.

2° au moyen d'un certificat qualifié au sens de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification ;

3° ou au moyen d'une copie de la carte d'identité du client dont la véracité est vérifiée par la consultation du Registre national.

La vérification peut également être effectuée au moyen d'une copie d'un document probant pour autant que l'identification soit opérée en vue de nouer une relation d'affaires, et pour autant que ni le client, ni la relation d'affaire ne présentent de risques particuliers de blanchiment de capitaux ou de financement du terrorisme.

36.- Carte d'identité électronique. S'agissant du recours à l'eID, la vérification correcte des données d'identification au départ du microprocesseur requiert une vérification électronique simultanée que les données figurant sur la puce sont signées électroniquement par le Registre National[85]. Il convient en outre de s'assurer que le certificat n'a pas été révoqué par celui-ci. Il est également recommandé dans ce cas que les procédures informatiques mises en œuvre soient conçues en manière telle que cette vérification soit opérée systématiquement et automatiquement, sans requérir d'intervention du préposé qui procède à l'identification, et sans qu'il ne dispose de la faculté de désactiver ce contrôle. Toutefois, nombre de pays ne disposent pas encore de carte d'identité électronique, et nombre d'utilisateurs ne sont pas non plus équipés en lecteurs de carte d'identité électronique.

S'agissant de l'admissibilité des certificats qualifiés d'identification, la Circulaire de la CBFA[86] précise qu'elle est soumise à diverses conditions liées aux caractéristiques du certificat : ne peuvent ainsi être admis que des « certificats qualifiés » requérant, pour être obtenus, une identification physique du titulaire, et qui n'ont pas été émis sous un pseudonyme. Des conditions d'admissibilité complémentaires sont également prévues s'agissant des qualités du prestataire de service de certification qui a émis le certificat.

Le règlement eIDAS, en harmonisant au niveau européen les exigences applicables aux certificats et en prévoyant leur reconnaissance entre États membres, devrait faciliter et harmoniser la mise en œuvre des mesures de vérification d'identité des clients quel que soit leur État membre d'origine, contribuant ainsi, non seulement à fournir des solutions sécurisées et fiables mais également à éliminer un obstacle majeur à la fourniture transfrontière de services financiers.

[85] Circulaire CBFA_2010_09 du 6 avril 2010 (modifiée).
[86] Circulaire CBFA_2010_09 du 6 avril 2010 (modifiée).

Dans le livre vert sur les services financiers de détail publié à Bruxelles, le 10 décembre 2015[87], la Commission européenne indiquait d'ailleurs que le Règlement eIDAS était prometteur car il « devrait permettre aux entreprises d'identifier plus facilement leurs clients à distance ou d'obtenir une authentification forte des parties aux opérations de paiement en application de la directive révisée sur les services de paiement. Dans ce contexte, le secteur financier est considéré comme l'un de ceux qui pourraient bénéficier le plus des solutions d'identification électronique. La marge d'amélioration dans ce domaine pourrait être considérable ».

En guise de conclusion

37.- Dématérialisation et besoin de confiance dans le domaine financier. Dans le secteur financier (comme dans d'autres domaines, d'ailleurs), la confiance constitue un élément absolument indispensable. Il en résulte notamment une exigence forte en termes d'identification et d'authentification des parties. Par ailleurs, dans la perspective d'une dématérialisation des échanges, les parties doivent être en mesure d'accomplir valablement diverses formalités principales (écrit, signature, mentions manuscrites, etc.) ou accessoires (horodatage, archivage, recommandé, etc.) dans l'environnement numérique.

À divers égards, le législateur est déjà intervenu. Par ailleurs, les acteurs du secteur suivent de près la question et, très tôt, des solutions techniques sécurisées ont été mises en œuvre.

38.- Quid avec eIDAS ? Avec le règlement eIDAS, la tendance devrait en tout cas se poursuivre, voire se renforcer, dans un cadre présentant un niveau plus élevé de sécurité juridique et technique, en ce Congrès, pour les opérations transfrontières. Il faut d'ailleurs espérer que le législateur veille à la cohérence et les renvois croisés entre les instruments adoptés. S'agissant par exemple de la DSP 2 et du règlement eIDAS, l'ABE, chargée de la définition du volet technique, semble être sensible à la mise en cohérence de l'ensemble.

L'existence d'un cadre normatif cohérent et aussi simple que possible est une condition nécessaire pour que des prestataires lancent des services de confiance, que ceux-ci soient exploités par les acteurs du secteur financier et, *in fine*, que les utilisateurs y recourent en toute confiance. Avec le règlement eIDAS, la voie semble bien tracée. Gageons que cela continue…

[87] http://eur-lex.europa.eu/legal-content/fr/TXT/?uri=CELEX%3A52015DC0630.